# Minneapolis
# Intelligent Operations Platform

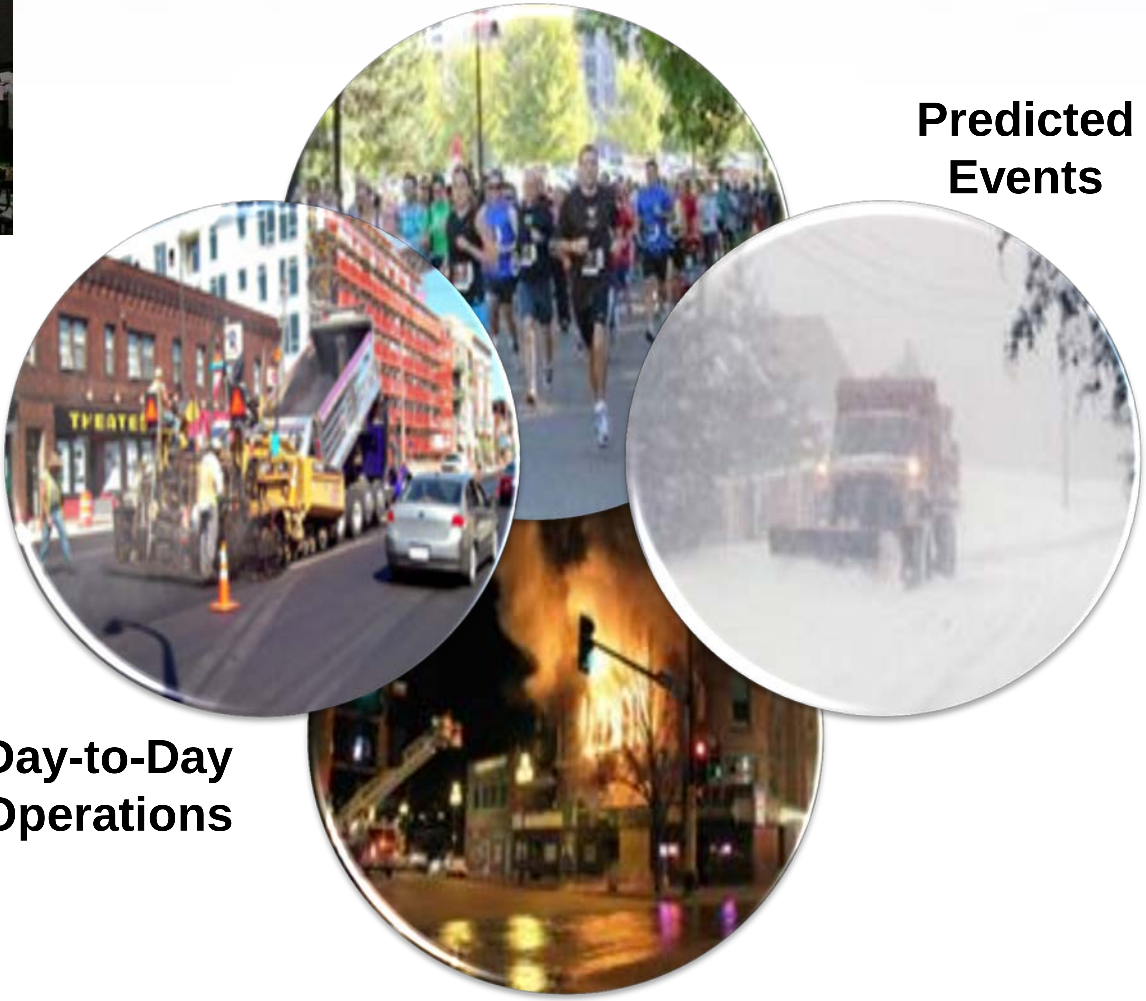
Pulse2014
The Premier Cloud Conference

February 23 – 26
MGM Grand – Las Vegas, Nevada

# Mission Control Focus

- □ Better coordinate city operations to gain efficiencies
- □ Deal more effectively with special events
- □ Improve handling of emergencies

## Manage Event Horizon



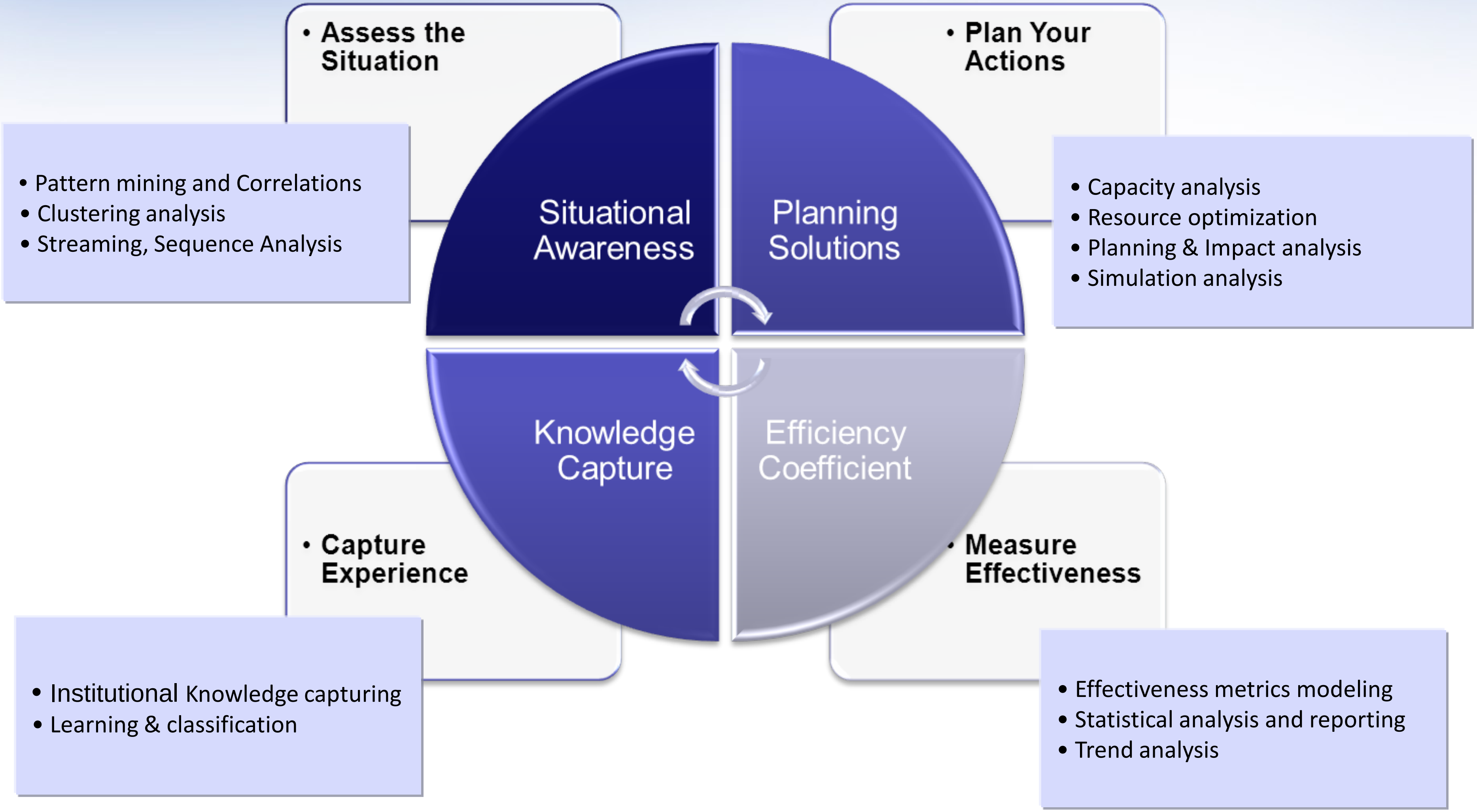
Normal Planned Events

Predicted Events

Day-to-Day Operations

Unplanned Events

# “Working” Functional Concept



- Assess the Situation

- Pattern mining and Correlations
- Clustering analysis
- Streaming, Sequence Analysis

- Plan Your Actions

- Capacity analysis
- Resource optimization
- Planning & Impact analysis
- Simulation analysis

- Capture Experience

- Institutional Knowledge capturing
- Learning & classification

- Measure Effectiveness

- Effectiveness metrics modeling
- Statistical analysis and reporting
- Trend analysis

# Customer Perspectives

- ❑ Residents / visitors
- ❑ Elected Officials
- ❑ Department leaders and employees

- ❑ Business view – Enterprise versus specific need(s)
- ❑ Geographic focus – City-wide versus specific geography (ward, precinct, etc.)
- ❑ Data visualized – map versus time

- ❑ Emphasizes value in having a product with generic, and thus, wide-spread application

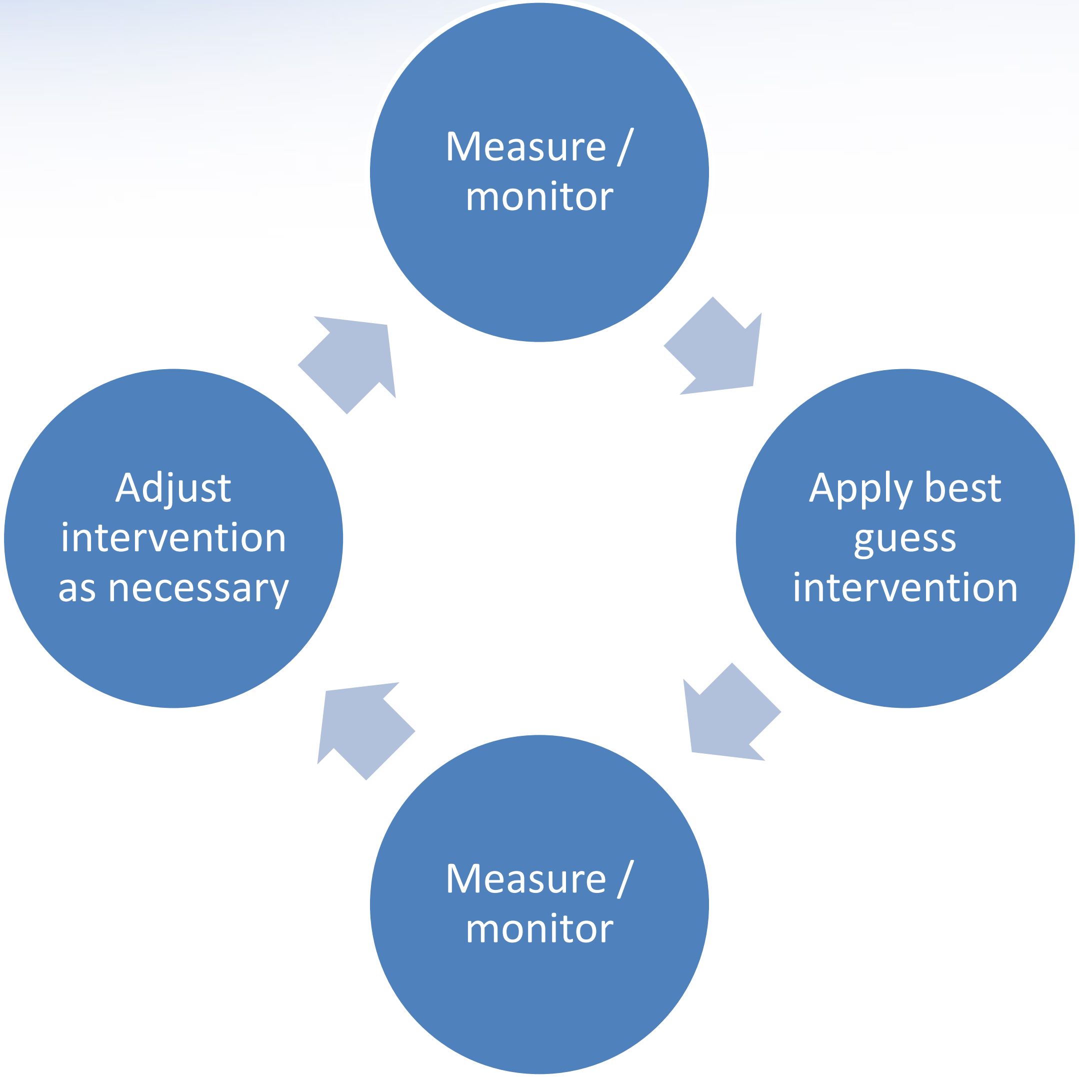
# Turning data into decisions

- ❑ Philosophy: Data → Information → Knowledge

- ❑ Largely focused on
  - ➢ Rear-view
  - ➢ Macro-geography with some exceptions
  - ➢ One dimensional (based on data from one department)

- ❑ Current City data-driven efforts
  - ➢ Police Code4
  - ➢ Results Minneapolis
  - ➢ Intelligent Operations Platform (IOP)

# Current approach



Measure / monitor

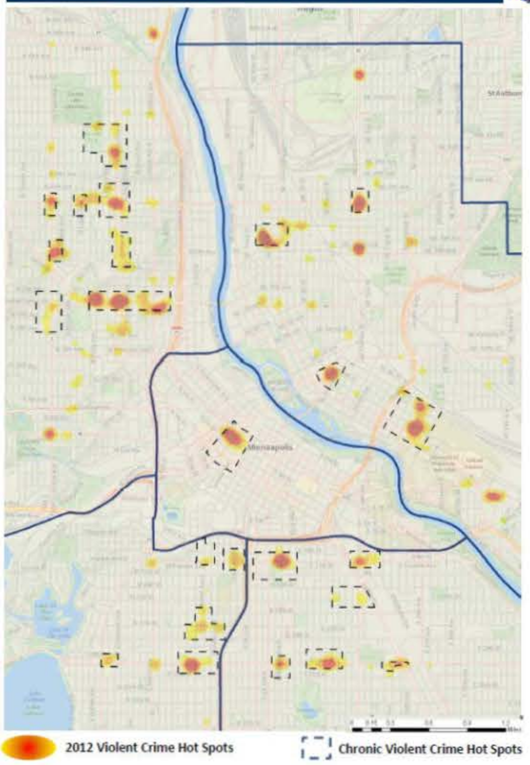
Apply best guess intervention

Measure / monitor

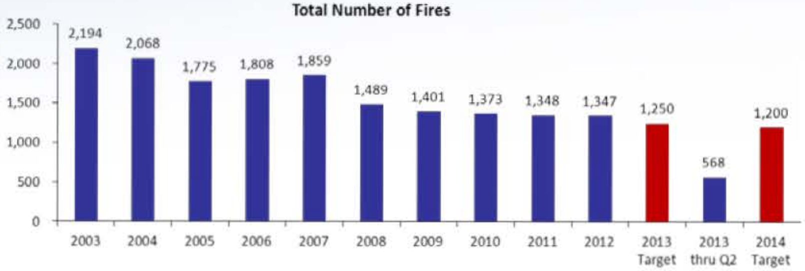
Adjust intervention as necessary

# What we get today

MINNEAPOLIS POLICE DEPARTMENT
Violent Crime Hot Spots in 2012

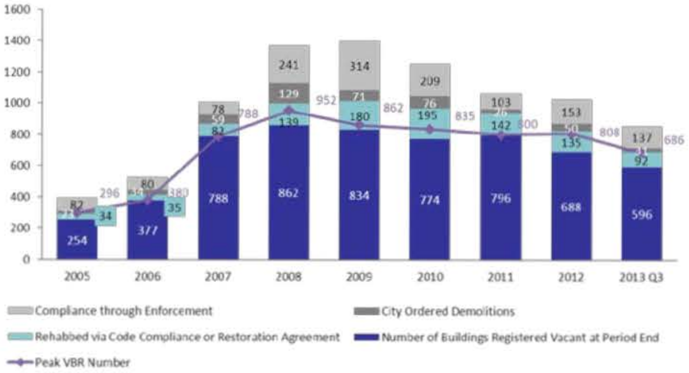


Total Number of Fires



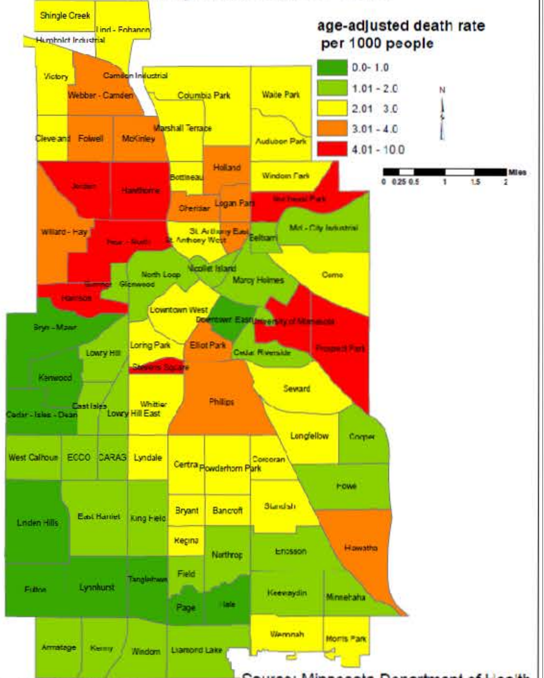
*Source: Minneapolis Fire Department: Firehouse, MFD-Incident Type*

Vacant Building Registration Activity



*Source: KIVA/COGNOS*

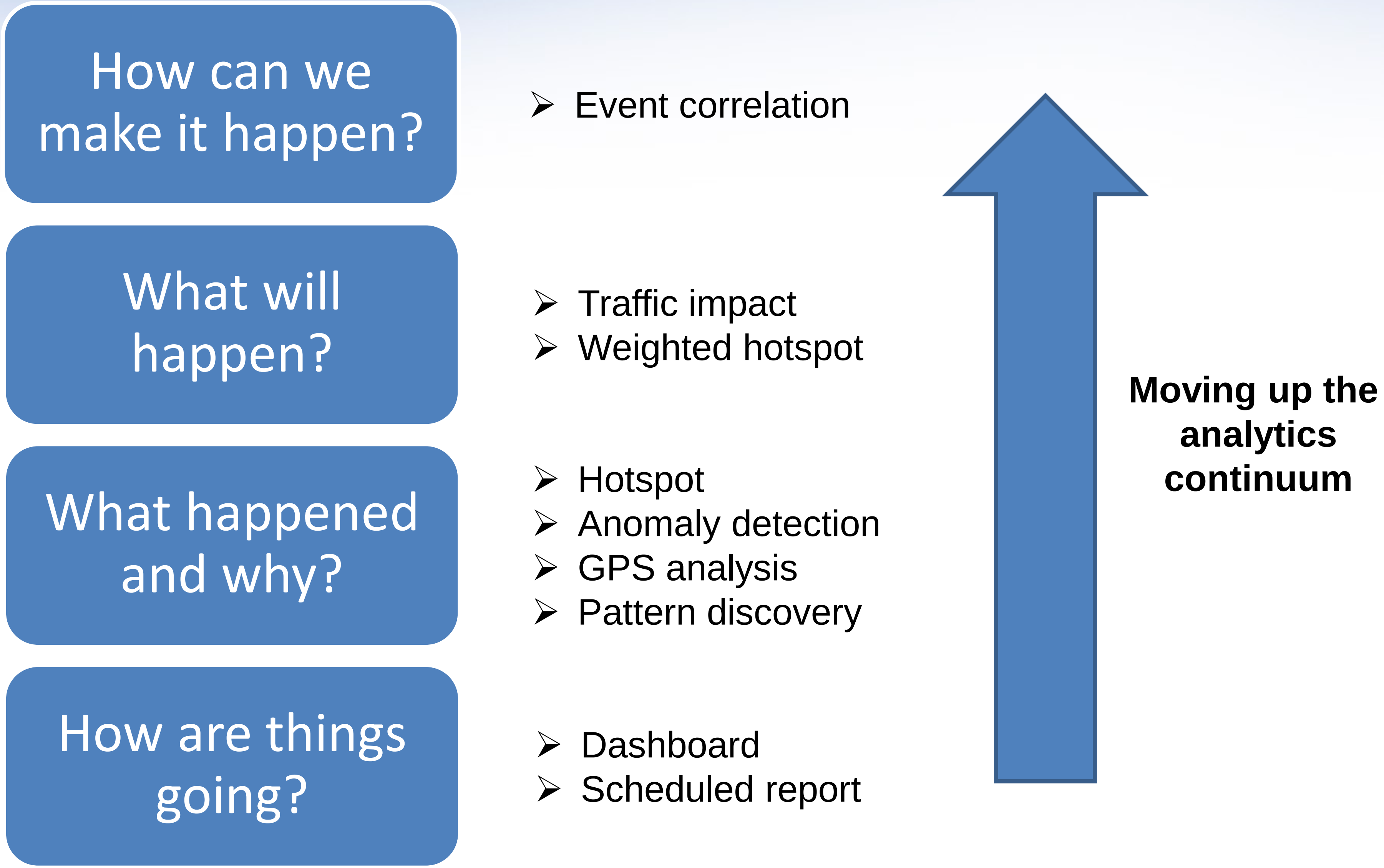
Age-adjusted annual premature ( 1-64) death rates by neighborhood, 2001-2010.



Created on : 01/07/13

Source: Minnesota Department of Health

# Future Approach



How can we make it happen?

- Event correlation

What will happen?

- Traffic impact
- Weighted hotspot

What happened and why?

- Hotspot
- Anomaly detection
- GPS analysis
- Pattern discovery

How are things going?

- Dashboard
- Scheduled report

**Moving up the analytics continuum**

# Benefits for Business

❑ Time savings (production, analysis, decisions, etc.)

❑ Thinking in 2,3,4,… dimensions, across enterprise

❑ Move up analytics continuum

❑ Better knowledge leading to better decision-making and better outcomes (zip codes and communities that are safe, livable, healthy, etc.)

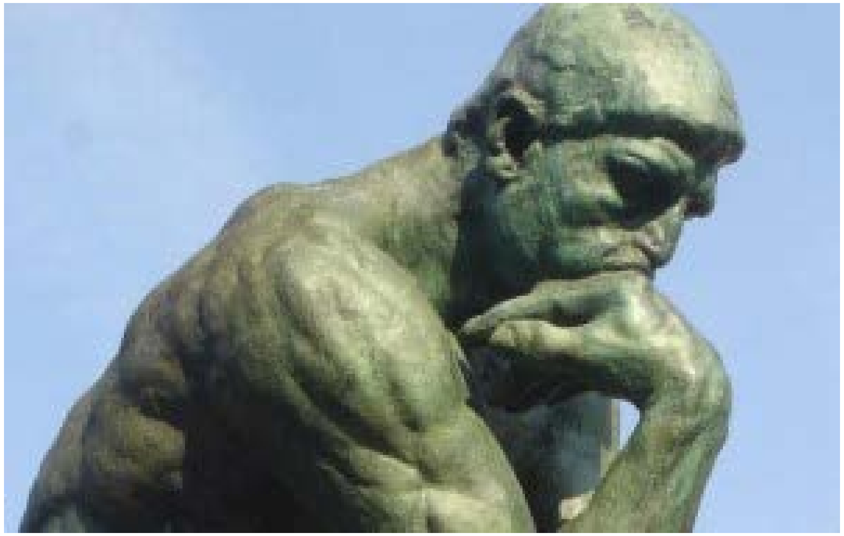
# Analytics is the Key

**Hotspot Detection**

**Workers search for places of more than usual interest, activity, or popularity**

**Event Correlation**

**Workers seek the cause that makes the effect happen**



**Pattern Discovery**

**Workers look for a reliable model of traits, acts, tendencies, or other observable characteristics of a person, group, or institution**

**Anomaly Detection**

**Workers look for deviations from the common rule, type, arrangement, or form**

# Use Case #1: Bad Landlords

**Hypothesis:** most housing issues are caused by a handful of landlords

## Challenge

- ❑ Who is a bad landlord?

## Technique

- ❑ Discover characteristics of a bad landlord through event correlation; compare against all landlords through pattern matching

# Use Case #2: Vacant Properties

**Hypothesis:** there is a tipping point where a concentration of vacant properties begins affecting the economic development of an area

## Challenge

- ❑ Which neighborhoods have vacant properties density affecting economic development?

## Technique

- ❑ Determine hotspots of vacant properties; compare surrounding area economics (assessed property values, business income, etc.) to like areas of city

# Use Case #3: Off Duty Officers

**Hypothesis:** when an event(s) overwhelms existing police resources, call upon off-duty officers working secondary security jobs

## Challenge

- ❑ Any off-duty officers available in area?

## Technique

- ❑ Store their locations across time

# Use Case #4: Rising Crime

**Hypothesis:** a specific criminal activity will often "catch on" within the criminal community

## Challenge

- ❑ What's causing spurt of burglaries?

## Technique

- ❑ Correlate events to crimes and/or discover patterns of activity

# Use Case #5: Public Events

**Hypothesis:** we can make the process of getting a permit more palatable

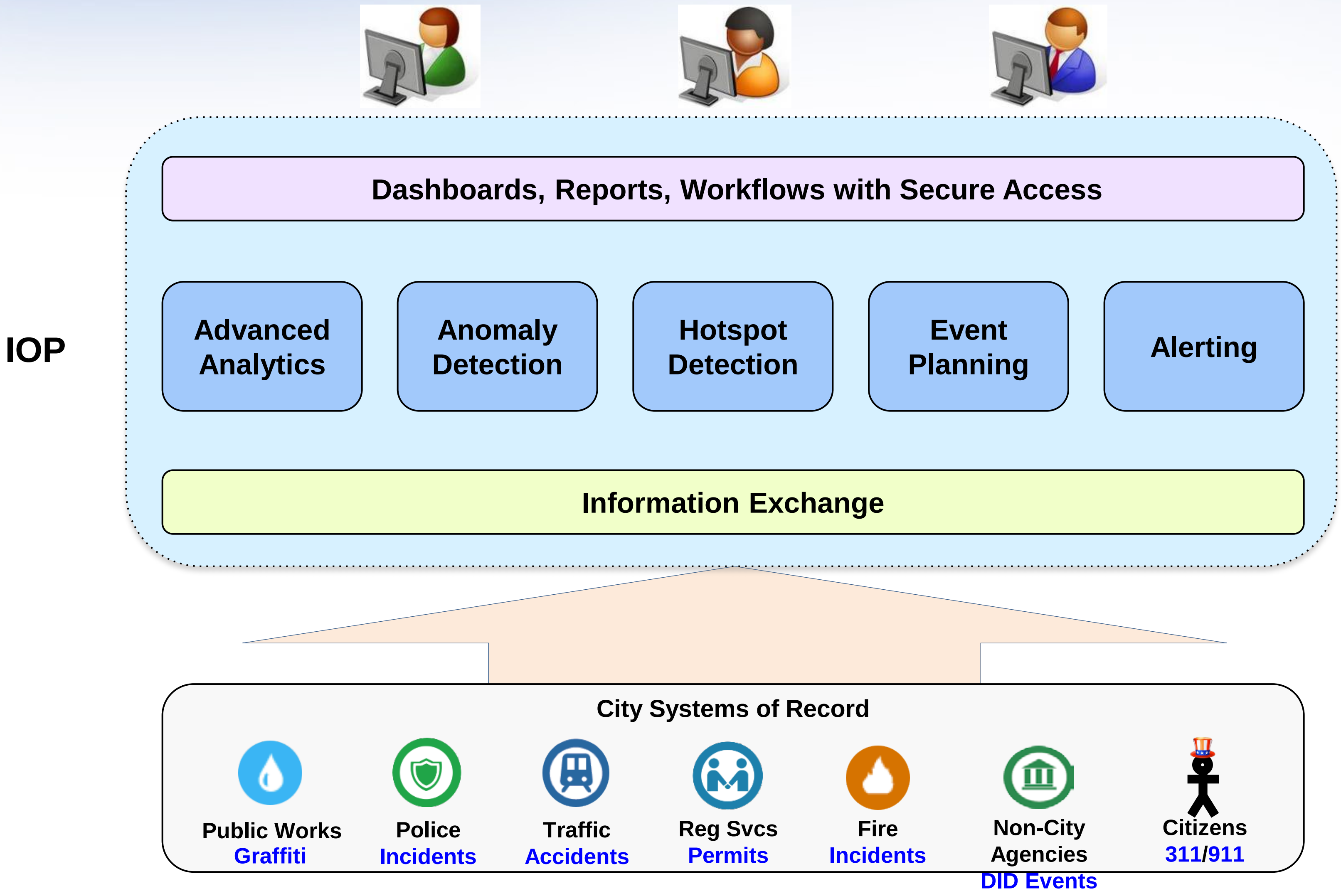
## Challenge

- ❑ Is the first week of next month a good time for a 5K run through the city?

## Technique

- ❑ Compare state-of-city on a given day

# Intelligent Operations Platform (IOP) – Improving City Operations



IOP

Dashboards, Reports, Workflows with Secure Access

Advanced Analytics

Anomaly Detection

Hotspot Detection

Event Planning

Alerting

Information Exchange

City Systems of Record

Public Works
Graffiti

Police
Incidents

Traffic
Accidents

Reg Svcs
Permits

Fire
Incidents

Non-City Agencies
DID Events

Citizens
311/911

Data Sources used for the City of Minneapolis implementation of IBM IOC

1) Lagan: 311 calls
2) Accident: a Public Works system used to record conditions detail of car accident. Focused on road conditions no driver information
3) Block Event: National Night Out event street closures
4) TritechCAD: 911 calls
5) Kiva: City's permitting system
6) CAPRS: Police incident records management system.
7) Govern: Assessor's Office system used to create the Estimate Market Value of properties

# Proposal For Work

# Juvenile Offender Modeling

Prepared for:

## Rochester Police Department

**Prepared By:**

Alpine Consulting
1100 East Woodfield Road
Schaumburg, IL 60173
Joe Siok, COO
Phone: 224.520.7500
E-mail: jsiok@alpineinc.com

**Confidential and Proprietary Information Notice**

This document contains confidential and proprietary information of Alpine Consulting, Inc. and is to be used for the sole purpose of permitting the recipient to evaluate Alpine's response. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose or distribute this information to any person outside the group directly responsible for evaluation of its contents without the expressed written permission of Alpine Consulting, Inc.

## Project Objectives

**Purpose**:

To introduce the potential of advanced analytics into the Rochester Police Department (RPD) Intelligence-Led Policing (ILP) initiative by building a working analytics model that demonstrates immediate organizational value, can be used for knowledge transfer, and will be a foundation for building new models in the future.

Specifically, IBM® SPSS® Modeler will be used to build a model(s) that will evaluate offender/offense relationships and patterns to determine a risk value, or equivalent, for juvenile offenders (age 14-17) as they pass into adulthood (age 18-21).

The implementation process will be used as an opportunity for knowledge transfer on building advanced analytics models and how to work with SPSS Modeler.

**Deliverables:**

- Juvenile offender analytics model and risk scores.
- Extract and consolidation applications.
- Output results suitable for presenting findings to project sponsors.
- Knowledge transfer of how to build a basic SPSS Model and SPSS Modeler.
- IBM-provided sample law enforcement model(s) for future use (as described in Project Tasks, (g) Training, below).
- Short and long-term infrastructure and licensing plan.

**In Scope:**

Historical law enforcement data extracts of criminal offenses (statutes, dates, supplemental and demographic characteristics) associated with each subject in the records system consolidated by ISII entity ID.

Analytics model that will determine trigger offenses and patterns of juvenile offenders and likelihood of career criminal behavior based on offender/offense relationships and patterns.

Leveraging IBM support resources and sample law enforcement models.

Risk score for juvenile offenders.

Knowledge transfer on building advanced analytics models and how to work with SPSS Modeler.

Compliance with Criminal Justice Information System (CJIS) requirements.

Infrastructure and software license plan that will support this project, position RPD for building and expanding future models and provide a longer-term roadmap for growth.

**Out of Scope:**

Consolidated offender and risk score.

Program for proactive enhanced enforcement target opportunities and intervention resource targeting.

Guarantees of resultant model suitability and effectiveness is out of scope. Alpine will make a best-effort attempt to find useful models, but we cannot guarantee the models will actually be useful.

Turning your staff into expert-level modelers is out of scope. Alpine's training will cover introductory modeling and related tool topics, but this provides only a beginning for RPD.

## Project Tasks

The following tasks will be performed:

(a) Project kickoff
(b) Software installation
(c) Data understanding
(d) Data preparation
(e) Modeling
(f) Reporting
(g) Training
(h) Implementation
(i) On-going support.

Project Kickoff. Communication is important for virtually every project. The initial steps will be undertaken to “get the ball rolling” and set up the communication. For example, a weekly meeting time will be determined.

Software Installation. Alpine will assist RPD with software installation, as needed.

Data Understanding. An analysis is only as good as the data which are provided (GIGO-garbage in, garbage out).

- Records for all individuals will be provided, including individual juvenile and adult information for offenders and non-offenders.
- Historical law enforcement data extracts of criminal offenses (statutes, dates, supplemental, and demographic characteristics) associated with each subject in the records system consolidated by ISII Entity ID.
- Additional fields (i.e., variables) will be considered (all that can be provided).
- A data dictionary/codebook or equivalent information will be provided that describes the data (e.g., meanings of codes–where appropriate, source, relationship, level, time period, measurement level, accuracy/quality).
- Assistance will be available in answering questions related to the data and project (e.g., discussion about file(s), variable(s), and purpose).
- The data will be handled in compliance with Criminal Justice Information System (CJIS) requirements.

Data Preparation. Significant effort in predictive modeling is devoted to preparation of data.

- The processing of the model will be done in batch mode (no real-time integration with source systems).
- The data file(s) will be consolidated before or within IBM® SPSS® Modeler.
- A data audit will be conducted for the variables.
- Automatic data preparation will be run to gain insight into the variables.
- As needed, variables may be adjusted (e.g., normalized and/or recoded).
- Additional variables may be generated from existing variables.

Modeling. Various analysis methods will be run to model juvenile offender risk score.

- Explore relationships between variables.
- Determine appropriate modeling techniques to use.
- Run, refine, and evaluate models.

Reporting. The results of the preliminary study will be presented. The presentation will be "layered" in that different levels of detail will be given (e.g., top-level, intermediate level).

Training. There will be a number of levels of training provided. These include:

- Alpine will provide assistance to IBM as they conduct their partial-day workshop on the law enforcement model that they have already produced for RPD.
- Alpine will provide a workshop that gives detail on the juvenile model development effort related to this project.
- Alpine will provide a two-day Introduction to IBM® SPSS® Modeler class using generic data for up to five participants.

Implementation. Alpine will provide a written procedure that analysts can use to apply the model. (The running of the model will be human-initiated; automation and scheduling is outside the scope of this project.)

On-Going Support. Alpine recommends that RPD establish a retainer, separate from this proposal in order to provide on-going SPSS mentoring and consulting (e.g., periodic juvenile model review and adjustment as well as creation of additional models).

## Project Overview/Estimates

Project Estimates

| **Approximate Estimate** | **Task** |
|---|---|
| 8 hours | Software installation |
| 16 hours | Data Understanding |
| 24 hours | Data Preparation |
| 32 hours | Modeling |
| 32 hours | Reporting and training |
| 16 hours | Implementation |
| 64 hours | Additional Time (as needed) |

Total ESTIMATED Hours: 192

NOTE: The above hours estimate per task are estimate ONLY. This is not a fixed bid project.

Travel Schedule. Work will be performed remotely when possible in order to help keep overall project costs down. On-site work is planned for four days at the beginning of the project for setting and obtaining the data and four days of on-site work is planned at the end of the project for presentation of results and training.

## Project Pricing

Pricing for this project will be charged on a per hour basis at a rate of $150.00 per hour (one-hundred fifty dollars per hour).

Alpine has estimated approximately 192 man hours. All work is to be billed on a time and materials basis.

Software will be quoted separately from this proposal and will be governed by the traditional IBM Passport Advantage agreement.

Terms of payment are Net 30, US Dollars. All other commercial terms will be governed by the Master Services Agreement previously executed.

An authorized signature on this page by the parties indicates their respective acceptance of this Statement of Work.

Agreed to:
**Rochester Police Department**
**101 4th Street SE**
**Rochester, MN  55904**

By: ______________________________
Authorized signature

Name:

Title:

Date:_________________________

Agreed to:
**Alpine Consulting, Inc.**
**1100 E. Woodfield Road**
**Suite 105**
**Schaumburg, IL  60173**
**United States**

By: ______________________________
Authorized signature

Name:

Title:

Date:________________________

# Plans to expand scope of license-plate readers alarm privacy advocates

Jun 17, 2014

Denise Green had just dropped off her sister at the 24th Street Mission BART station after picking her up from the hospital.

Green, who was driving a 1992 red Lexus, noticed a San Francisco police car with its lights on pull up behind her as she passed through the intersection of Mission Street and Highland Avenue. Green pulled over to let the patrol car pass.

She was stunned when officers yelled, "Put your hands up!"

Sgt. Ja Han Kim ordered her to step out of the car, and as Green complied, she turned and saw several officers with their guns trained on her.

"Don't look at us!" one of them said.

"Turn around!" the officers shouted, forcing Green to her knees.

They handcuffed her and searched her Lexus. Green overheard officers standing near her license plate shouting numbers to each other.

"It's not a seven?" one said.

"No, three five zero," another officer replied.

Denise Green has filed a lawsuit against San Francisco police over a 2009 traffic stop in which her car was mistakenly identified as stolen.

Green, a Muni driver and 50-year-old San Francisco resident, had been pulled over and detained because her car was mistakenly identified as a stolen vehicle by an automatic license-plate reader the city had installed on its police cars. The officers did not confirm her license plate with their dispatcher.

"It was a nightmare," Green said of the traffic stop. "I had no idea what was going on or why they were treating me like a criminal – I just hope that never happens to anyone else."

Five years later, as Green's lawsuit over the incident goes to a civil trial this year, the use of license-plate readers has emerged as one of the biggest concerns among privacy advocates. Car-tracking technology is becoming ubiquitous in cities around the United States, and the types of data collected and analyzed with the help of license-plate readers is expanding into other realms of personal information.

Documents obtained by The Center for Investigative Reporting show that a leading maker of license-plate readers wants to merge the vehicle identification technology with other sources of identifying information, alarming privacy advocates. Vigilant Solutions is pushing a system that eventually could help fuse public records, license plates and facial recognition databases for police in the field.

The Livermore, California, company released its own facial recognition software last year for use in stationary and mobile devices. The technology uses algorithms to determine whether a person's face matches that of somebody already in a law enforcement database. Like license-plate readers, facial recognition technology has been criticized for incorrectly identifying people.

Vigilant also is the market leader in license-plate data collection. The company runs the Law Enforcement Archive and Reporting Network database, which stores more than 2.5 billion records and adds roughly 70 million new license-plate scans monthly. The company offers law enforcement free access to its license-plate data through another database, the National Vehicle Location Service.

Vigilant has faced criticism from the public, privacy advocates and lawmakers in California for working behind the scenes to rally police and sheriff's departments to its side – including prohibiting law enforcement officials from talking to the media about its products without its approval.

FYI

From: Rich Neumeister

# Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates June 14, 2014 Center for Investigative Reporting

Vigilant Solutions offers free access to license-plate reader, or LPR, data to law enforcement. It is the market leader in this data collection.

**Credit:** Vigilant Solutions presentation

A Vigilant PowerPoint presentation about its products, obtained by CIR, contains a section on the "near future" for the company. That includes a fusion of public records, license-plate data and facial recognition, according to the slide. Another technology, dubbed MOAB, would help law enforcement find vehicles using a "probabilistic assessment" of a vehicle's location based on historical data and public records.

Another slide prepared for Texas law enforcement shows how a combined data program could work. It would pull mug shots from the local Department of Motor Vehicles database and notify law enforcement with an alert if "a vehicle is associated with someone with a known criminal history." The slide also describes "facial images embedded into" the license-plate record. Another describes how Vigilant's FaceSearch application works on mobile devices.

Amy Widdowson, a Vigilant spokeswoman, said the slides reviewed by CIR were of a prototype program that did not actually include facial recognition technology.

As for specific references to merging license-plate data with facial recognition and public records, Widdowson said the slide "is merely showing that law enforcement can combine data from public records with LPR (license-plate reader) data to reduce their search area for a suspect."

Last week, Vigilant announced a new product it called Mobile Companion, which the company said was "driven by a desire" to combine license-plate data with facial recognition technology "into a very nice and easy-to-use mobile application."

Privacy advocates said combining historical plate-reader data with public records and facial recognition technology runs contrary to law enforcement's argument that license plates are not considered personally identifying information.

Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, which is suing the Los Angeles County Sheriff's Department and Los Angeles Police Department for information about their collection and use of license-plate data, said Vigilant's plans could represent a sea change in the technology.

Noting that Vigilant already offers analytical software that traces the movements of a vehicle through the public and private plate-reader data it retains, Lynch said the company's plans could pose a threat to individual privacy.

By combining the location data from license-plate readers with public records such as court files and property records – as well as photographs of individuals from criminal or DMV databases – into one search tool, which in turn could be used with facial recognition software, license-plate readers could move into uncharted territory.

A plate reader could tag a passing car and the names of people associated with the vehicle and keep a log of where that person traveled. That data potentially could be stored for months or years.

"When you're combining data from multiple sources, it becomes incredibly revealing," Lynch said.

Facial recognition technology is making rapid advances. The National Security Agency is reportedly mining intercepted communications, the Internet and foreign government databases for images used to identify individuals of interest to the intelligence agency. Along with its own in-house facial recognition program, the NSA also uses software made by a Google subsidiary, PittPatt.

For her part, Green filed a civil suit against the San Francisco Police Department. The case is expected to go to trial this winter after the 9th Circuit Court of Appeals overturned a lower court's decision to dismiss her claim. At the time of the incident, San Francisco police used license-plate readers manufactured by PIPS Technology, a subsidiary of Federal Signal Corp., not technology from Vigilant Solutions.

San Francisco officials declined to comment on the pending litigation.

Green's attorney, Michael Haddad, said the incident took a serious toll on her. "It was extremely terrifying, and Denise ended up having to miss a couple weeks of work and get counseling afterwards."

But Haddad noted one significant fact in the documentation for the trial: The machines can have an error rate as high as 8 percent. "There's some acknowledgment by the manufacturers," he said, "that there's a significant percentage of the time that they're wrong."

**Managing Vigilant's public image**

Meanwhile, Vigilant has been working behind the scenes to shield its technology from public view and manage the public perception of its products.

An agreement between Vigilant and the Ontario Police Department in San Bernardino County, California, for example, prohibits the department from publishing material about Vigilant's technology or cooperating with journalists who ask questions about the plate-reader system – without first obtaining the company's consent.

"Agency agrees not to use proprietary materials or information in any manner that is disparaging," according to the agreement. The police department agreed "not to voluntarily provide ANY information, including interviews, related to Vigilant, its products or its services to any member of the media without the express written consent of Vigilant."

Terry Francke, a public records expert and general counsel for open-government group Californians Aware, said such agreements violate the state Public Records Act. Information related to public contracts and services, Francke said, "are public records, and the government may not withhold them to comply with the contractor's wishes."

As it faced legislation this year that would curb its business, Vigilant and law enforcement joined forces even further. The California District Attorneys Association, California State Sheriffs' Association and California Police Chiefs Association all submitted letters opposing legislation that would have curbed Vigilant's practices.

The California legislation would have banned public and private entities from selling license-plate data, required privacy policies for agencies using the technology and prevented license-plate data from being the sole basis for search warrants. The legislation was watered down significantly from a previous version that would have restricted law enforcement's retention of license-plate data to five years.

During its campaign, Vigilant canvassed its law enforcement customers for anecdotal evidence of successful investigations using license-plate readers to lobby against the bill, which was defeated May 29 in the state Senate, according to emails obtained through the Public Records Act.

A mass email on Feb. 2 from Brian Shockley, Vigilant Solutions' vice president for marketing, to subscribers claimed that the now-defeated legislation, SB 893, "would completely eliminate the ability for Vigilant to collect and share its license plate reader data with you."

The email also makes clear Vigilant's aggressive stance toward government regulation of its business. Shockley wrote that "government should not be legislating away law enforcement's right to this tool that is helping to solve major crimes and protect the public. The focus should not be on who collects the data or how long it is stored, the focus should be on proper access controls, proper use and protections against misuse."

Widdowson, the Vigilant spokeswoman, said the email was sent to Vigilant law enforcement customers because the company "feels it is important to inform our law enforcement customers about pending legislation that can negatively impact their ability to protect and serve."

Vigilant sells license-plate readers to over a dozen California agencies, including the California Highway Patrol, Orange County Sheriff's Department, and the Sacramento Police and County Sheriff's departments. For its business with law enforcement in the city of Alameda, Anaheim, Marin County, San Rafael and Sacramento, Vigilant won the contracts without going through a competitive bidding process.

In Utah, Vigilant and a subsidiary company, Digital Recognition Network, are suing the state in civil court to block regulations passed by the state Legislature last year on license-plate readers. In Massachusetts, Vigilant is lobbying heavily against pending legislation that would restrict law enforcement agencies' retention of license-plate data to a matter of days.

Widdowson said concerns about how long data is kept is "a red herring," declaring that the Legislature should instead focus on "access control and enforcing existing laws." No law currently regulates the use of license-plate data in California for public or private entities.

State Sen. Jerry Hill, D-San Mateo, author of the California legislation, said law enforcement continued to lobby against the bill even after it was amended to restrict the use of license-plate data by private entities. He said that reflects on what he calls the "incestuous relationship" between license-plate reader companies and public safety agencies.

"Vigilant has been able to leverage public safety and California law enforcement for their own financial gain by holding out the ability to access their information at no charge," Hill said. "That enticement is the reason law enforcement opposed the bill."

From: Rich Neumeister

# Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates  June 14, 2014  Center for Investigative Reporting

Denise Green had just dropped off her sister at the 24th Street Mission BART station after picking her up from the hospital.

Green, who was driving a 1992 red Lexus, noticed a San Francisco police car with its lights on pull up behind her as she passed through the intersection of Mission Street and Highland Avenue. Green pulled over to let the patrol car pass.

She was stunned when officers yelled, “Put your hands up!”

Sgt. Ja Han Kim ordered her to step out of the car, and as Green complied, she turned and saw several officers with their guns trained on her.

“Don’t look at us!” one of them said.

“Turn around!” the officers shouted, forcing Green to her knees.

They handcuffed her and searched her Lexus. Green overheard officers standing near her license plate shouting numbers to each other.

“It's not a seven?” one said.

“No, three five zero,” another officer replied.

Green, a Muni driver and 50-year-old San Francisco resident, had been pulled over and detained because her car was mistakenly identified as a stolen vehicle by an automatic license-plate reader the city had installed on its police cars. The officers did not confirm her license plate with their dispatcher.

“It was a nightmare,” Green said of the traffic stop. “I had no idea what was going on or why they were treating me like a criminal – I just hope that never happens to anyone else.”

Five years later, as Green’s lawsuit over the incident goes to a civil trial this year, the use of license-plate readers has emerged as one of the biggest concerns among privacy advocates. Car-tracking technology is becoming ubiquitous in cities around the United States, and the types of data collected and analyzed with the help of license-plate readers is expanding into other realms of personal information.

A Vigilant PowerPoint presentation about its products, obtained by CIR, contains a section on the "near future" for the company. That includes a fusion of public records, license-plate data and facial recognition, according to the slide. Another technology, dubbed MOAB, would help law enforcement find vehicles using a "probabilistic assessment" of a vehicle's location based on historical data and public records.

Another slide prepared for Texas law enforcement shows how a combined data program could work. It would pull mug shots from the local Department of Motor Vehicles database and notify law enforcement with an alert if "a vehicle is associated with someone with a known criminal history." The slide also describes "facial images embedded into" the license-plate record. Another describes how Vigilant's FaceSearch application works on mobile devices.

Amy Widdowson, a Vigilant spokeswoman, said the slides reviewed by CIR were of a prototype program that did not actually include facial recognition technology.

As for specific references to merging license-plate data with facial recognition and public records, Widdowson said the slide "is merely showing that law enforcement can combine data from public records with LPR (license-plate reader) data to reduce their search area for a suspect."

Last week, Vigilant announced a new product it called Mobile Companion, which the company said was "driven by a desire" to combine license-plate data with facial recognition technology "into a very nice and easy-to-use mobile application."

Privacy advocates said combining historical plate-reader data with public records and facial recognition technology runs contrary to law enforcement's argument that license plates are not considered personally identifying information.

Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation, which is suing the Los Angeles County Sheriff's Department and Los Angeles Police Department for information about their collection and use of license-plate data, said Vigilant's plans could represent a sea change in the technology.

Noting that Vigilant already offers analytical software that traces the movements of a vehicle through the public and private plate-reader data it retains, Lynch said the company's plans could pose a threat to individual privacy.

By combining the location data from license-plate readers with public records such as court files and property records – as well as photographs of individuals from criminal or DMV databases – into one search tool, which in turn could be used with facial recognition software, license-plate readers could move into uncharted territory.

A plate reader could tag a passing car and the names of people associated with the vehicle and keep a log of where that person traveled. That data potentially could be stored for months or years.

"When you're combining data from multiple sources, it becomes incredibly revealing," Lynch said.

Facial recognition technology is making rapid advances. The National Security Agency is reportedly mining intercepted communications, the Internet and foreign government databases for images used to identify individuals of interest to the intelligence agency. Along with its own in-house facial recognition program, the NSA also uses software made by a Google subsidiary, PittPatt.

For her part, Green filed a civil suit against the San Francisco Police Department. The case is expected to go to trial this winter after the 9th Circuit Court of Appeals overturned a lower court's decision to dismiss her claim. At the time of the incident, San Francisco police used license-plate readers manufactured by PIPS Technology, a subsidiary of Federal Signal Corp., not technology from Vigilant Solutions.

San Francisco officials declined to comment on the pending litigation.

Green's attorney, Michael Haddad, said the incident took a serious toll on her. "It was extremely terrifying, and Denise ended up having to miss a couple weeks of work and get counseling afterwards."

But Haddad noted one significant fact in the documentation for the trial: The machines can have an error rate as high as 8 percent. "There's some acknowledgment by the manufacturers," he said, "that there's a significant percentage of the time that they're wrong."

**Managing Vigilant's public image**

Meanwhile, Vigilant has been working behind the scenes to shield its technology from public view and manage the public perception of its products.

An agreement between Vigilant and the Ontario Police Department in San Bernardino County, California, for example, prohibits the department from publishing material about Vigilant's technology or cooperating with journalists who ask questions about the plate-reader system – without first obtaining the company's consent.

"Agency agrees not to use proprietary materials or information in any manner that is disparaging," according to the agreement. The police department agreed "not to voluntarily provide ANY information, including interviews, related to Vigilant, its products or its services to any member of the media without the express written consent of Vigilant."

Terry Francke, a public records expert and general counsel for open-government group Californians Aware, said such agreements violate the state Public Records Act. Information related to public contracts and services, Francke said, "are public records, and the government may not withhold them to comply with the contractor's wishes."

As it faced legislation this year that would curb its business, Vigilant and law enforcement joined forces even further. The California District Attorneys Association, California State Sheriffs' Association and California Police Chiefs Association all submitted letters opposing legislation that would have curbed Vigilant's practices.

The California legislation would have banned public and private entities from selling license-plate data, required privacy policies for agencies using the technology and prevented license-plate data from being the sole basis for search warrants. The legislation was watered down significantly from a previous version that would have restricted law enforcement's retention of license-plate data to five years.

During its campaign, Vigilant canvassed its law enforcement customers for anecdotal evidence of successful investigations using license-plate readers to lobby against the bill, which was defeated May 29 in the state Senate, according to emails obtained through the Public Records Act.

A mass email on Feb. 2 from Brian Shockley, Vigilant Solutions' vice president for marketing, to subscribers claimed that the now-defeated legislation, SB 893, "would completely eliminate the ability for Vigilant to collect and share its license plate reader data with you."

The email also makes clear Vigilant's aggressive stance toward government regulation of its business. Shockley wrote that "government should not be legislating away law enforcement's right to this tool that is helping to solve major crimes and protect the public. The focus should not be on who collects the data or how long it is stored, the focus should be on proper access controls, proper use and protections against misuse."

Widdowson, the Vigilant spokeswoman, said the email was sent to Vigilant law enforcement customers because the company "feels it is important to inform our law enforcement customers about pending legislation that can negatively impact their ability to protect and serve."

Vigilant sells license-plate readers to over a dozen California agencies, including the California Highway Patrol, Orange County Sheriff's Department, and the Sacramento Police and County Sheriff's departments. For its business with law enforcement in the city of Alameda, Anaheim, Marin County, San Rafael and Sacramento, Vigilant won the contracts without going through a competitive bidding process.

In Utah, Vigilant and a subsidiary company, Digital Recognition Network, are suing the state in civil court to block regulations passed by the state Legislature last year on license-plate readers. In Massachusetts, Vigilant is lobbying heavily against pending legislation that would restrict law enforcement agencies' retention of license-plate data to a matter of days.

Widdowson said concerns about how long data is kept is "a red herring," declaring that the Legislature should instead focus on "access control and enforcing existing laws." No law currently regulates the use of license-plate data in California for public or private entities.

State Sen. Jerry Hill, D-San Mateo, author of the California legislation, said law enforcement continued to lobby against the bill even after it was amended to restrict the use of license-plate data by private entities. He said that reflects on what he calls the "incestuous relationship" between license-plate reader companies and public safety agencies.

“Vigilant has been able to leverage public safety and California law enforcement for their own financial gain by holding out the ability to access their information at no charge,” Hill said. “That enticement is the reason law enforcement opposed the bill.”

# 7 mass surveillance tools your local police might be using

May 06, 2014

Kelly Chen
News Engagement Specialist

READ THIS LATER SHARE

Investigation(s):
State of Surveillance

Topic(s):
Business and Technology
Money and Politics
National Security

If you've been concerning yourself with the Heartbleed bug and the National Security Agency, you might as well have these seven items on your radar, too. Military-inspired technologies are coming home for use by local law enforcement.

Since 2001, federal grants from the Department of Homeland Security have been trickling to local authorities for counterterrorism efforts. But even years after 9/11, these agencies are shopping around for military-inspired surveillance tools that can keep watch on average citizens.

The rise of a surveillance state has raised questions about the legality of how law enforcement agencies acquire new technologies and inform the public of their use. Individual searches and seizures are protected under the Fourth Amendment, but laws addressing mass surveillance of the public are few and limited.

The Center for Investigative Reporting continues to uncover how technology is revolutionizing the way we're being policed and what that means for our civil liberties. (Quick nonprofit plug: Back our Beacon Reader campaign to help sustain our reporting on this issue).

Here are some examples of surveillance technology that's already in use:

## 1. Wide-area surveillance

CIR and KQED discovered that the Los Angeles County Sheriff's Department conducted a two-week experiment that attached cameras to a manned civilian aircraft (not a drone) without telling Compton residents. CIR reporter G.W. Schulz described it as "Google Earth with a rewind button and the ability to play back the movement of cars and people as they scurry about the city."

## 2. Facial recognition software

How facial recognition works

Military-grade facial recognition software has landed in San Diego County. Using a tablet, police

MORE COVERAGE

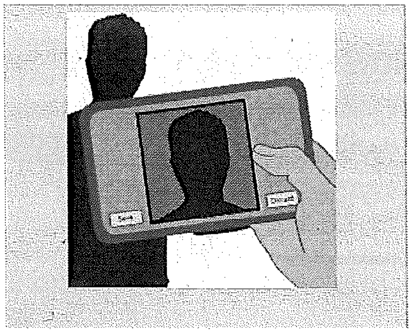
+ More from the blog

+ State of Surveillance

RELATED

- Help us keep an eye on the agencies watching you
- Find CIR on Reddit for more on local surveillance
- Hollywood-style surveillance technology inches closer to reality

**Read more: State of Surveillance**



Click to view the full graphic.

can take a photo of your face and run it against a database of about 348,000 county arrestees. This pilot program also rolled out without any public hearing or notice.

### 3. License-plate scanners

A license-plate reader mounted on a San Leandro Police Department car can log thousands of plates in an eight-hour patrol shift. "It works 100 times better than driving around looking for license plates with our eyes," says police Lt. Randall Brandt.
**Credit:** Michael Katz-Lacabe

While not a new technology, the increasing use of license-plate scanners is raising serious concerns about how that data is stored and who has access to it. One manufacturer, Vigilant Solutions, which also houses a massive private database of plate information, makes law enforcement agencies sign nondisclosure agreements.

### 4. Streetlights with recording capabilities

In Las Vegas, officials are using ordinary-looking streetlights with many talents. These Intellistreets, as they're called by designer Illuminating Concepts, run on wireless Internet and can come equipped with add-ons that would allow you to record and shoot video. As of 2013, Las Vegas officials say they are not using these features – they just have the ability to do so.

### 5. Behavioral recognition software

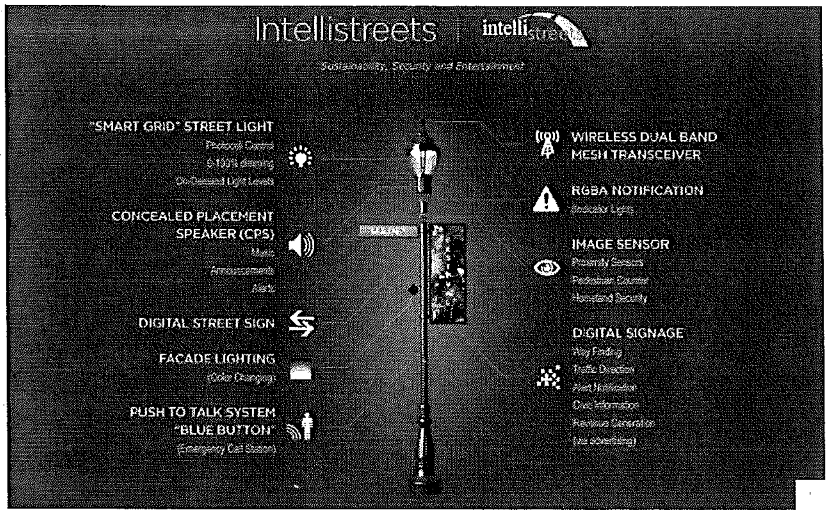
During the 2012 Republican National Convention in Tampa, Florida, police used behavioral recognition software to amp up surveillance and security. The software uses camera footage to automate suspicious activity detection. To fight back, Jon Gales created an app to track where the cameras were located.

### 6. Stingray

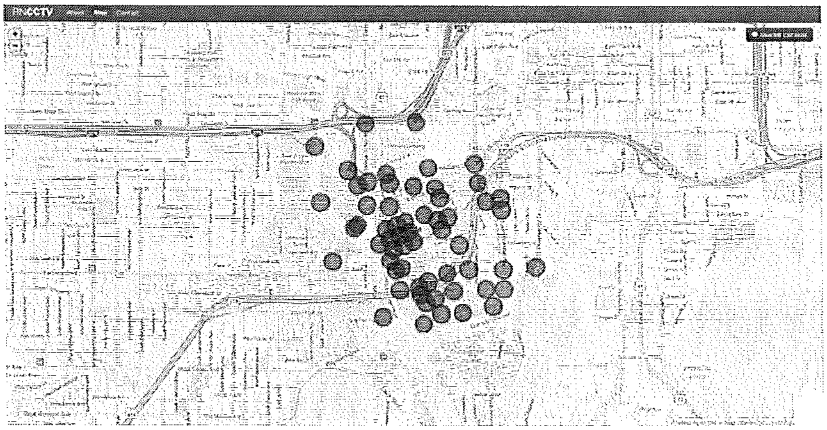
In California, multiple local agencies from the Bay Area to Sacramento have been using stingray technology to track and collect cellphone data in real time with precision. The ACLU describes a stingray as "a device that mimics a cell tower and thereby tricks all wireless devices on the same network into communicating with it." News10 in Sacramento tried to find out which agencies in particular are using the device – all refused to disclose how they were using it, and some would not comment on whether they have it.

### 7. Intelligence analysis software

The Los Angeles Police Department already is using intelligence analysis tools from Palantir, a Silicon Valley-based firm that makes data-mining software and is partially funded by the CIA. The department did not



**Credit:** Illuminating Concepts screen shot



**Credit:** RNCCTV screen shot

comment on its use of the intelligence program to LA Weekly, but officials explain how they use Palantir on a daily basis in a video testimonial:

*Donate to CIR's new Beacon Reader campaign to support our work on this issue. Follow us on Twitter and Facebook and subscribe to our newsletters.*

*Like our content? Help us do more.* SUPPORT US

LEAVE A COMMENT

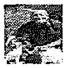
Login or signup

**You must be logged in to comment**

Type your comment here...

Post

Live



GregoryGeyer

there are other surveillance tools that personally have seen...these are like little stars that actually look like stars in the distance, but they are not. they control them and you didn't know it, they hear and see everything

Last Month from californiawatch · Reply

VIA TWITTER

Live

No items at this time...

About Contact Press Privacy Policy Ethics Guide Job Opportunities **Reporter Tools** **Shop** Connect with CIR: **Email Alerts** **Twitter** **Facebook** **Tumblr** **RSS**